applied sciences

MDPI

Article

A Novel Mobile Communications Authentication Scheme with Roaming Service and User Anonymity

Kai Chain [1], Wen-Chung Kuo [2,*] and Jiin-Chiou Cheng [3]

[1] Department of Computer and Information Science, Republic of China Military Academy, Kaohsiung 83059, Taiwan; chainkai@mail2000.com.tw

[2] Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology, Number 123 University Road, Section 3, Douliou, Yunlin 64002, Taiwan

[3] Department of Computer Science and Information Engineering, Southern Taiwan University of Science and Technology, Tainan 71005, Taiwan; chiou@mail.stust.edu.tw

* Correspondence: simonkuo@yuntech.edu.tw; Tel.: +886-5-534-2601 (ext. 4515); Fax: +886-5-531-2170

Academic Editors: Wen-Hsiang Hsieh and Christos Bouras
Received: 13 September 2016; Accepted: 24 November 2016; Published: 30 November 2016

Abstract: Many novel, effective, and efficient applications and networking services are being developed for the Social Internet of Things. Recently, Li proposed a more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications. The security analysis and discussion of the agreement phase is sufficiently safe; however, an attacker can intercept the identity of a mobile user's home agent in the authentication phase. By using this information, the attacker can mount distributed denial-of-service attacks in the roaming phase through replay attacks targeting the network's foreign agent and mobile user's home agent by using their corresponding session keys. Li's method also has some shortcomings regarding anonymity that we aim to address. To overcome these issues, this study proposes an elliptic curve–based wireless roaming anonymous login method for the authentication phase. The problems faced in the roaming phase are resolved, and this approach provides balanced session key computation between senders and receivers. Burrows-Abadi-Needham logic (BAN-logic) is used to verify the security of the proposed scheme. The proposed scheme affords good security, efficiency, and integrity and maintains anonymity.

Keywords: roaming; anonymity; mutual authentication; elliptic curve discrete logarithm problem; wireless networks; BAN-logic

1. Introduction

Wireless networks and smartphones have undergone rapid developments, allowing the use of the same device across different networks [1,2]. Users such as businessmen or tourists visiting a new area can use a smart card to register with their home agents. Such cards use an anonymous connection to register to the home agent from the foreign agent server [3,4]. After validation, a temporary certificate is sent to the user. The user may use this temporary certificate for network roaming via the foreign agent server. This approach can provide billing information while maintaining anonymity [5–8].

In general, an anonymous roaming scheme has three entities: mobile user (MU), foreign agent (FA), and home agent (HA) [9–13]. In communication, the user must remain anonymous to the other entities. This scheme consists of three phases: registration (initialization phase), authentication (first phase), and roaming (second phase) [14–16]. When an MU is anonymously roaming in a foreign network, it can use one of two methods: real-time online and offline. Real-time online means that when a user requests roaming permissions, the FA can immediately authenticate with the HA and verify the user's legitimacy. The FA is unaware of the user's true identity but only knows whether the user is legitimate.

Offline means that when the user requests roaming permissions, the FA can verify the user's legitimacy directly through the information obtained during the registration phase. In other words, this method does not use a real-time connection with the HA to verify the user, and the FA does not know the user's true identity [17–23]. In this study, the mobile phone roaming anonymous login is based on the real-time online method.

In 2004, Zhu and Ma [24] first proposed an authentication scheme with anonymity for wireless environments. Although they claimed that their scheme was secure, some weaknesses remained. The attacker can obtain r ($r = H(N||ID_{HA}) \oplus H(N||ID_{MU}) \oplus ID_{HA} \oplus ID_{MU}$) by registering and calculating the HA's private key or by intercepting messages n of other legitimate users and then using the HA's private key exclusive—or r can obtain the legitimate user's identity ID_{MU} and PW_{MU}. In other words, this scheme does not provide anonymity. In 2006, however, Lee et al. [25] showed several security flaws in Zhu and Ma's scheme and then improved it. Unfortunately, the HA still provided PW_{MU} to the MU in the registration phase, enabling PW_{MU} to be calculated. In 2008, Wan et al. [13] noted the security vulnerabilities of Lee et al.'s scheme and proposed an enhanced version of their scheme. However, in 2009, Chang and Lee [26] showed that Wu et al.'s improved scheme still did not provide anonymity, as they claimed. Recently, in 2012, Li [27] proposed a more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications. This scheme's main characteristic is that the MU chooses PW_{MU} in the registration phase and sends it to the HA to perform other operations. Because the MU sends PW_{MU} to the HA, this solves the ID_{MU} and PW_{MU} problems encountered in traditional schemes. Li's scheme is more efficient in terms of performance because it uses a lightweight elliptic curve Diffie-Hellman computation compared with traditional schemes that use RSA (Ron Rivest, Adi Shamir, and Leonard Adlema) [28] with certificates. However, Li's scheme has two weaknesses: (1) ID_{HA} is transmitted using plaintext in the authentication phase and therefore an attacker can easily perform distributed denial-of-service attacks if ID_{HA} is intercepted; and (2) there exist some issues in how the session key is generated in the roaming phase. Specifically, the details of session key management are not shown and are left unaddressed in Li's scheme [27].

This study proposes an elliptic curve–based authentication scheme with roaming service and user anonymity for mobile communications that overcomes the weaknesses of Li's scheme [27] and ensures fair load-sharing of the session key computation in the authentication phase.

The remainder of this paper is organized as follows: In Section 2, we review Li's scheme and analyze its weaknesses. In Section 3, we propose an elliptic-curve-based authentication scheme with roaming service and user anonymity for mobile communications. In Section 4, we use BAN-logic (Burrows-Abadi-Needham logic) to demonstrate the security of our proposed scheme. In Section 5, we analyze our proposed scheme, and in Section 6, we compare it with other schemes. Finally, Section 7 presents the conclusions of our study.

2. Preliminaries

In this section, we review Li's scheme [27]. His scheme consists of three phases: registration, authentication, and roaming, of which the authentication phase is real-time online.

2.1. Li's Scheme

For simplicity, we list the common notations used throughout Li's scheme in Table 1.

Table 1. Notations used throughout Li's scheme.

Notations	Descriptions
MU	A mobile user
HA	The home agent of a mobile user
FA	The foreign agent of the network
ID_{MU}	The MU's identity
PW_{MU}	The MU's password
N	A strong secret key of the HA
T_A	Timestamp generated by an entity A
$Cert_A$	Certificate of an entity A
$(X)_K$	Encryption of a message X using a symmetric key K
(P_A,S_A)	The asymmetric public key and private key pair of an entity A based on Elliptic curve cryptography (ECC)
E_P	An elliptic curve equation, over a finite field p: $y^2 = x^3 + ax + b \bmod p$, where $p > 2^{16\circ}$, $n > 2^{160}$, a and b are two integer elements and $4a^3 + 27b^2 \bmod p \neq 0$
E	An elliptic curve equation of HA choose
p, n	Two large prime numbers
P	A base point with the order n over E
SK_{HF}	A pre-shared symmetric key between HA and FA
$\oplus$	Exclusive-OR (XOR) operation
H(.)	A collision-free one-way hash function
$\mid\mid$	Concatenation

2.1.1. Registration Phase

R1. MU→HA: $m_{LR1}\{ID_{MU}, H(PW_{MU}\oplus r_n)\}$

The MU chooses the identity ID_{MU}, password PW_{MU}, and a random number r_n; calculates $H(PW_{MU}\oplus r_n)$; and sends the registration request message $\{ID_{MU}, H(PW_{MU}\oplus r_n)\}$ to the HA.

R2. HA→MU: $m_{LR2}\{ID_{HA}, E_p, E, n, P, P_{HA}, z, H(.)\}$

When the registration request message $\{ID_{MU}, H(PW_{MU}\oplus r_n)\}$ is received from the MU, the HA calculates $H(ID_{MU}\mid\mid N)$ and $z = H(PW_{MU}\oplus r_n)\oplus H(ID_{MU}\mid\mid N)$. Then, the HA sends ID_{HA}, E_p, E, n, P, P_{HA}, z, and H(.) to the MU.

R3. MU: $ID_{HA}, E_p, E, n, P, P_{HA}, z, H(.)$

After the message $\{ID_{HA}, E_p, E, n, P, P_{HA}, z, H(.)\}$ is received from the HA, the MU stores this information along with r_n onto the smart card. This completes the registration phase.

2.1.2. Authentication Phase

V1. MU→FA: $m_{LV1}\{X, IND, c_1, ID_{HA}, T_{MU}\}$

When the MU enters ID_{MU} and PW_{MU}, the smart card chooses a random number x and calculates $X = xP$, $X_1 = xP_{HA}$, $Z = z\oplus H(PW_{MU}\oplus r_n)$, $IND = ID_{MU}\oplus H(X_1\mid\mid T_{MU})$, and $c_1 = H(X_1\mid\mid Z)$. T_{MU} is the MU's current timestamp. Then, the MU sends the authentication request message $\{X, IND, c_1, ID_{HA}, T_{MU}\}$ to the FA.

V2. FA→HA: $m_{LV2}\{X, IND, c_1, Y, T_{MU}, T_{FA}, MAC_{FA}\}$

When the authentication message is received from the MU, the FA checks the validity of the timestamp T_{MU}. If it is valid, FA chooses a random number y and calculates $Y = yP$ and $MAC_{FA} = H(X\mid\mid IND\mid\mid c_1\mid\mid Y\mid\mid T_{MU}\mid\mid T_{FA}\mid\mid SK_{HF})$, where T_{FA} is the FA's current timestamp and SK_{HF} is a session key between the HA and the FA. The FA then sends the message $\{X, IND, c_1, Y, T_{MU}, T_{FA}, MAC_{FA}\}$ to the HA.

V3. HA→FA: $m_{LV3}\{MAC_{HA}, c'_2 = c_2\oplus H(T_{HA}\mid\mid SK_{HF}), T_{HA}\}$

When the authentication message is received from the FA, the HA checks the validity of the timestamp T_{FA}. If it is valid, the HA calculates $H(X\mid\mid IND\mid\mid c_1\mid\mid Y\mid\mid T_{MU}\mid\mid T_{FA}\mid\mid SK_{HF})$ and verifies whether $H(X||IND||c_1||Y||T_{MU}||T_{FA}||SK_{HF})$ is the same as the received MAC_{FA}. If it is not valid, the HA terminates the execution. Otherwise, the HA calculates $X'_1 = XN$, $ID'_{MU} = IND \oplus H(X'_1||T_{MU})$, and $c'_1 = H(X'_1||H(ID'_{MU}||N))$ and checks whether the equation $c'_1 = c_1$ holds. If it is not valid, the HA terminates the execution. Otherwise, the HA calculates $MAC_{HA} = H(X||Y||ID_{FA}||ID_{HA}||T_{HA}||SK_{HF})$ and $c_2 = H(X'_1||H(ID'_{MU}||N)||X||Y||ID_{FA}||ID_{HA})$, where T_{HA} is the HA's current timestamp. The HA then sends the message $\{MAC_{HA}, c'_2 = c_2 \oplus H(T_{HA}||SK_{HF}), T_{HA}\}$ to the FA.

V4. FA→MU: $m_{LV4}\{Y, c_2, c_3 = (TCert_{MU})_{sk}\}$

When the message is received from the HA, the FA checks the validity of the timestamp T_{HA}. If it is valid, the FA calculates $H(X||Y||ID_{FA}||ID_{HA}||T_{HA}||SK_{HF})$ and verifies whether $H(X||Y||ID_{FA}||ID_{HA}||T_{HA}||SK_{HF})$ is the same as the received MAC_{HA}. If it is not valid, the FA terminates the execution. Otherwise, the FA believes that the HA is a valid home agent and the MU is an authenticated user. The FA then calculates $c_2 = c'_2 \oplus H(T_{HA}||SK_{HF})$ and a session key $sk = yX = xyP$ and sends the message $\{Y, c_2, c_3 = (TCert_{MU})_{sk}\}$ to the MU, where $TCert_{MU}$ is a temporary certificate for the MU.

V5. MU: $Y, c_2, c_3 = (TCert_{MU})_{sk}$

When a message is received from the FA, the MU calculates $H(X'_1||H(ID'_{MU}||N)||X||Y||ID_{FA}||ID_{HA})$ and verifies whether it is the same as the received c_2. If it is not valid, the MU terminates the execution. Otherwise, the MU believes that it is communicating with a legal FA. The MU subsequently calculates a session key $sk' = xY = xyP = sk$ and decrypts c_3. Finally, the MU obtains $TCert_{MU}$ from the FA.

2.1.3. Roaming Phase

L1. MU→FA: $m_{LRo1}\{m_i, mac\}$

The MU calculates $m_i = (TCert_{MU}||sk_{i+1}||Other)_{ski}$ and $mac = H(TCert_{MU}||sk_{i+1}||Other)$ and sends the roaming message $\{m_i, mac\}$ to the FA, where sk_{i+1} is a session key for the next communication.

L2. FA: m_i, mac

When received the roaming message from the MU, the FA calculates the session key and decrypts m_i. The FA then checks the validity of mac. If it is valid, the FA updates the session key sk_i with sk_{i+1} for the next communication.

2.2. Advantages of Li's Scheme

Li's scheme has two advantages. First, the MU calculates $H(PW_{MU} \oplus r_n)$ and sends this message to HA. In other words, the MU chooses PW_{MU} and sends it to the HA; this prevents PW_{MU} from being calculated easily, which was a shortcoming of previous schemes. Second, Li's scheme is more efficient in terms of performance because it uses the lightweight elliptic curve Diffie-Hellman computation compared with other traditional schemes that use heavyweight asymmetric cryptosystems with certificates.

2.3. Weaknesses of Li's Scheme

Li's scheme has two weaknesses. First, because ID_{HA} is not properly hidden, an attacker can easily intercept it and determine the relationships among the MU, FA, and HA. In addition, it does not use an authentication mechanism between the MU and the FA, and therefore, for any message m_1 to the FA, the FA performs the appropriate processing and transfers the results to HA. Because of this feature, the attacker can flood a specific target (HA), intercept other people's message (m_1) over the wireless network, and change the message timestamp T_{MU}. Although the message will not be verified through the HA, the attacker can do enough to cripple a specific target host (HA), namely, the attacker can perform a distributed denial-of-service attack. Second, Li's scheme does not clearly define or address some important issues, such as the assignment of session key computation during the roaming phase and how to manage the various session keys for a large number of users. If there are hundreds of thousands of people in a wireless network environment, and each person's session key is different, managing the keys is not trivial. Table 2 shows a detailed description of the weaknesses of Li's scheme [18].

Table 2. Weaknesses of Li's scheme.

Step	Phase	Descriptions
V1	Authentication phase	Because ID_{HA} is transmitted in plaintext, the attacker can intercept messages and determine the relationship among the MU, FA, and HA. Then, the attacker can use a replay attack and target a specific object, namely the HA, by a distributed denial-of-service attack.
L2	Roaming phase	Li's scheme does not clearly explain how to obtain corresponding session keys and the relationship between different users. So FA is impossible for a user to calculate the specific session key, and decrypt m_i. Therefore, this scheme lacks integrity.

3. Proposed Scheme

The proposed scheme consists of three phases: registration, authentication, and roaming, of which the authentication phase is real-time online.

3.1. Notations

The proposed scheme uses the same notations as those in Table 1 and the new notations listed in Table 3.

Table 3. Additional notations.

Notations	Descriptions
P_{FA} = b	A public key of the FA based on ECC
G_1	**Additive group** on ECC
G_2	**Multiplicative group** on ECC
H_1	$H_1 = \{0,1\}^* \rightarrow Z^*q$
H_2	$H_2 = \{0,1\}^n \rightarrow Z^nq$
H_3	$H_3 = G_1 \rightarrow \{0,1\}^*$

3.2. Registration Phase

Figure 1 shows the registration phase of the proposed scheme. The detailed steps as follows.

R1. MU→HA: $m_{R1}\{ID_{MU}, H_2(PW_{MU} \oplus r_n)\}$

The MU chooses ID_{MU}, PW_{MU}, and a random number r_n and calculates $H_2(PW_{MU} \oplus r_n)$. Then, the MU sends the message $\{ID_{MU}, H_2(PW_{MU} \oplus r_n)\}$ to the HA.

R2. HA→MU: $m_{R2}\{ID_{HA}, E_p, E, n, P, P_{HA}, z_i, H(.), W_i\}$

When the message $H_2(PW_{MU} \oplus r_n)$ is received from the MU, the HA calculates $z_i = H_2(PW_{MU} \oplus r_n) \oplus H_1(ID_{MU}||N||W_i) \oplus H_3(W_i)$. Then, the HA chooses a random number w, calculates $W_i = wP$, and transmits $\{ID_{HA}, E_p, E, n, P, P_{HA}, z_i, W_i, H(.)\}$ to the MU.

R3. MU: ID_{HA}, E_p, E, n, P, P_{HA}, z_i, W_i, H(.)

The MU enters W_i into his/her smart card, and the MU's smart card contains ID_{HA}, E_p, E, n, P, P_{HA}, z_i, W_i, and H(.)

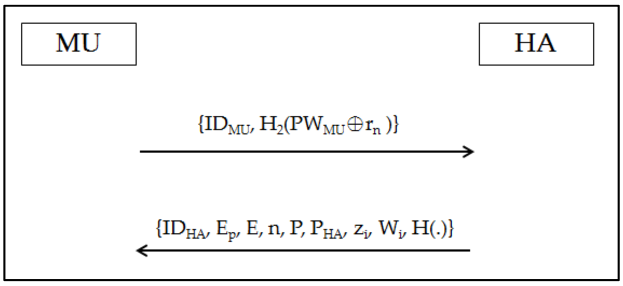
MU
HA
{ID_{MU}, $H_2(PW_{MU}\oplus r_n)$}
{ID_{HA}, E_p, E, n, P, P_{HA}, z_i, W_i, H(.)}

Figure 1. Registration phase.

3.3. Authentication Phase

Figure 2 shows the authentication phase of the proposed scheme. The steps are detailed as follows.

V1. MU→FA: $m_{V1}\{A, U\}$

The U inserts the smart card into the card reader and enters ID_{MU} and PW_{MU}. Then, the smart card chooses a random number x and calculates $X = xP$, $X_1 = xP_{HA}$, $ZP = [z_i\oplus H_2(PW_{MU}\oplus r_n)\oplus H_3(W_i)]P$, $IND = ID_{MU}\oplus H_1(X_1||T_{MU})$, $c_1 = H(X_1||Z)$, and $A = aP$, where T_{MU} is the MU's timestamp. Subsequently, the MU calculates a shared key $EC = aY = ayP$, the message $U = (W_i, X, IND, c_1, ID_{HA}, T_{MU})_{EC}$, and sends an authentication request message {A, U} to the FA.

V2. FA→HA: $m_{V2}\{W_i, X, IND, c_1, Y, T_{MU}, T_{FA}, MAC_{FA}\}$

The FA calculates a shared key $yA = ayP = EC$ and decrypts U by using EC to obtain W_i, X, IND, c_1, Y, and T_{MU}. Then, the FA checks the validity of the timestamp T_{MU}. If it holds, the FA chooses a random number y and calculates $Y = yP$ and $MAC_{FA} = H_1(W_i||X||IND||c_1||Y||T_{MU}||T_{FA}||SK_{HF})$, where T_{FA} is the FA's current timestamp and SK_{HF} is the session key between the HA and the FA. This key is mainly used for signature verification. The FA then sends the message $\{W_i, X, IND, c_1, Y, T_{MU}, T_{FA}, MAC_{FA}\}$ to the HA.

V3. HA→FA: $m_{V3}\{MAC_{HA}, MAC'_{HA} = MAC_{HA}\oplus H_1(T_{HA}||SK_{HF}), T_{HA}\}$

The HA checks the validity of the timestamp T_{FA}. If it is valid, the HA checks if the calculated value $MAC'_{FA} = H_1(W_i||X|| IND||c_1||Y||T_{MU}||T_{FA}||SK_{HF})$ is the same as the received MAC_{FA}. If it is not valid, the HA terminates the execution. Otherwise, the HA calculates $X'_1 = XN$, $ID'_{MU} = IND\oplus H_1(X'_1||T_{MU})$, and $c'_1 = H_1(X'_1||H_1(ID'_{MU}||N||W_i))$ and checks whether the equation $c'_1 = c_1$ holds. If it is not valid, the HA terminates the execution. Otherwise, the HA calculates $MAC_{HA} = H_1(W_i||X||Y||ID_{FA}||ID_{HA}||T_{HA}||SK_{HF})$, where T_{HA} is the HA's current timestamp. The HA then sends the message $\{MAC_{HA}, MAC'_{HA} = MAC_{HA}\oplus H_1(T_{HA}||SK_{HF}), T_{HA}\}$ to the FA.

V4. FA→MU: $m_{V4}\{c_2 = (TCert_{MU})_{sk}\}$

The HA checks the validity of the timestamp T_{HA}. If it is valid, the FA calculates $MAC_{HA} = H_1(W_i||X||Y||ID_{FA}||ID_{HA}||T_{HA}||SK_{HF})$ and verifies whether this value is the same as the received MAC_{HA}. If it is not valid, the FA terminates the execution. Otherwise, the FA believes that the MU is an authenticated user. The FA then calculates $MAC_{HA} = MAC'_{HA}\oplus H_1(T_{HA}||SK_{HF})$, $Y = yP$, and $sk = yX = xyP$ and sends the message $\{c_2 = (TCert_{MU})_{sk}\}$ to the MU, where $TCert_{MU}$ is a temporary certificate from the FA to the MU.

V5. MU: Y, $c_2 = (TCert_{MU})_{sk}$

The MU calculates a session key $sk' = xY = xyP = sk$ and decrypts c_2. Finally, the MU obtains $TCert_{MU}$ from the FA.

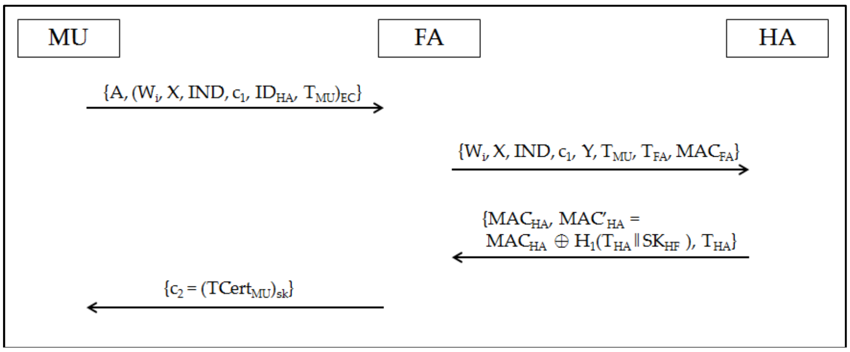
MU
FA
HA
{A, (W$_i$, X, IND, c$_1$, ID$_{HA}$, T$_{MU}$)$_{EC}$}
{W$_i$, X, IND, c$_1$, Y, T$_{MU}$, T$_{FA}$, MAC$_{FA}$}
{MAC$_{HA}$, MAC′$_{HA}$ =
MAC$_{HA}$ ⊕ H$_1$(T$_{HA}$‖SK$_{HF}$), T$_{HA}$}
{c$_2$ = (TCert$_{MU}$)$_{sk}$}

Figure 2. Authentication phase.

3.4. Roaming Phase

Figure 3 shows the roaming phase of the proposed scheme. The steps are detailed as follows.

L1. MU→FA: $m_{Ro1}\{A, U\}$

The MU calculates $m_i = (TCert_{MU}||sk_{i+1}||Other)_{sk_i}$, $mac = H(TCert_{MU}||sk_{i+1}||Other)$, and $(m_i||mac||sk_i||T_{MU})_{EC}$ and sends the message {A, U} to the FA, where sk_{i+1} is a session key for the next communication and T_{MU} is the current timestamp.

L2. FA: A, U

The FA calculates aA = abP = EC and decrypts U to obtain m_i, mac, sk_i, and T_{MU}. The FA then checks the validity of T_{MU}. If it is valid, the FA decrypts m_i by using sk_i and calculates $mac' = H(TCert_{MU}||sk_{i+1}||Other)$. If the equation mac′ = mac holds, the FA updates the session key sk_i with sk_{i+1} for the next communication.

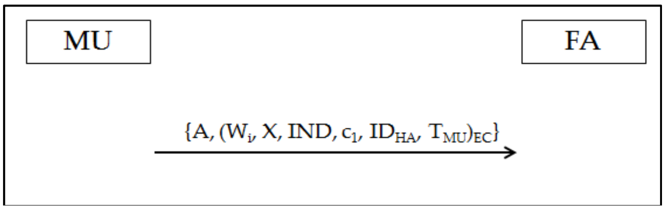

Figure 3. Roaming phase.

4. BAN-Logic Analysis

4.1. Introduction to BAN-Logic

BAN-logic is used to establish session key security between the MU and the FA to prove that the session key is safeguarded in the authentication phase of our scheme. The main process has four proofs:

a. MU believes the session key: MU←-SK-→FA
b. MU believes that FA believed the session key: MU←-SK-→FA
c. A believes the session key: MU←-SK-→FA
d. FA believes that MU believed the session key: MU←-SK-→FA

According to the BAN-logic characteristics of the security analysis, the following basic symbolic representation rules are used [29–31]:

1. (X, Y): X or Y is one part of the parameter (X, Y).

2. <X>Y: X can be obtained through the secret parameter Y.
3. $\{X\}_K$: X is encrypted under the key K.
4. P$\leftarrow$-K-$\rightarrow$Q: P and Q may use the shared secret key K to communicate. The third party does not know the secret key K.
5. P<=S=>Q: S is only known between P and Q. P and Q must use S to prove the identity of each other.

4.2. Rules of BAN-Logic

Freshness rule: If part of the message is fresh, then the whole message is also fresh.

Message meaning rule: K is a key shared between P and Q; therefore, if P sees an encrypted message, it must come from Q.

Nonce verification rule: If P believes that Q once said X, then P believes that Q once believed X. If X is fresh, then Q should still hold this belief.

Jurisdiction rule: If P trusts Q as an authority on X, then P should believe X if Q does so.

4.3. Authentication Proof Based on BAN-logic

We use the rules of BAN-logic to represent the authentication phase in our proposed scheme and describe these messages as follows:

1. m_{V1}. MU$\rightarrow$FA: $\{(<ID_{MU}>_{H_1(X_1||T_{MU})}, <X_1, H_1(ID_{MU}||N||W_i)>_{H_2(PW_{MU}\oplus r_n), H_3(W_i)}, W_i, X, ID_{HA})\}_{EC}$
2. m_{V2}. FA$\rightarrow$HA: $(<ID_{MU}>_{H_1(X_1||T_{MU})}, <X_1, H_1(ID_{MU}||N||W_i)>_{H_2(PW_{MU}\oplus r_n), H_3(W_i)}, W_i, X, Y)_{\{R_i\}SK_{HF}}$
3. m_{V3}. HA$\rightarrow$FA: $\{(W_i, X, Y, ID_{HA}, ID_{FA})\}_{SK_{HF}}$
4. m_{V4}. FA$\rightarrow$MU:$\{TCert_{MU}\}_{<MU\leftarrow -SK-\rightarrow FA>}$

To analyze our proposed scheme, we made the following assumptions without loss of generality:

A1: MU believes X.
A2: MU believes X_1.
A3: MU believes A.
A4: FA believes Y.
A5: FA believes R_i.
A6: HA believes W_i.
A7: MU believes MU<=$^{H(N)}$=>HA.
A8: HA believes MU<=$^{H(N)}$=>HA.
A9: FA believes FA <=$^{SK}{}_{HF}$=>HA.
A10: HA believes FA <=$^{SK}{}_{HF}$=>HA.
A11: MU believes MU$\leftarrow$-^{SK}-$\rightarrow$FA.
A12: FA believes (MU controls MU$\leftarrow$-^{SK}-$\rightarrow$FA).
A13: HA believes (MU controls MU$\leftarrow$-^{SK}-$\rightarrow$FA).
A14: HA believes (MU controls ID_{MU}).
A15: ID_{MU} is known only to user.
A16: MU believes $TCert_{MU}$.
A17: MU believes ID_{MU}.
A18: FA believes ID_{FA}.
A19: HA believes ID_{HA}.

We show the processes of the proofs as follows:

1. By m_{V1}, A3, and A4, we apply the freshness rule to derive

$$\text{FA believes} \\ (<ID_{MU}>_{H_1(X_1||T_{MU})}, <X_1, H_1(ID_{MU}||N||W_i)>_{H_2(PW_{MU}\oplus r_n), H_3(W_i)}, W_i, X, ID_{HA}). \qquad \text{(Statement 1)}$$

2. By m_{V1}, A1, and A6, we apply the nonce verification rule to derive

$$\begin{gathered}\text{FA believes that MU said}\\ (<ID_{MU}>_{H_1(X_1||T_{MU})}, <X_1, H_1(ID_{MU}||N||W_i)>_{H_2(PW_{MU}\oplus r_n), H_3(W_i)}, ID_{HA}).\end{gathered} \tag{Statement 2}$$

3. By m_{V2} and A10, we apply the message meaning rule to derive

$$\begin{gathered}\text{HA believes that FA said}\\ (<ID_{MU}>_{H_1(X_1||T_{MU})}, <X_1, H_1(ID_{MU}||N||W_i)>_{H_2(PW_{MU}\oplus r_n), H_3(W_i)}, W_i, X, Y)_{\{R_i\}}.\end{gathered} \tag{Statement 3}$$

4. By m_{V2}, A1, A4, A5, and A6, we apply the nonce verification rule to derive

$$\begin{gathered}\text{HA believes that FA believes}\\ (<ID_{MU}>_{H_1(X_1||T_{MU})}, <X_1, H_1(ID_{MU}||N||W_i)>_{H_2(PW_{MU}\oplus r_n), H_3(W_i)}).\end{gathered} \tag{Statement 4}$$

5. By Statement 4, we break the conjunction to obtain

$$\text{HA believes that FA believes } <ID_{MU}>_{H_1(X_1||T_{MU})}. \tag{Statement 5}$$

$$\text{HA believes that FA believes } <X_1, H_1(ID_{MU}||N||W_i)>_{H_2(PW_{MU}\oplus r_n), H_3(W_i)}. \tag{Statement 6}$$

6. By Statement 5 and A2, we apply the message meaning rule and nonce verification rule to derive

$$\text{HA believes that MU believes } ID_{MU}. \tag{Statement 7}$$

7. By Statement 7 and A14, we apply the jurisdiction rule to obtain

$$\text{HA believes } ID_{MU}. \tag{Statement 8}$$

8. By Statement 8 and A15, we break the conjunction to obtain

$$\text{HA believes } MU <= ID_{MU} => HA. \tag{Statement 9}$$

9. By m_{V3} and A9, we apply the message meaning rule to derive

$$\text{FA believes that HA said } (W_i, X, Y, ID_{HA}, ID_{FA}). \tag{Statement 10}$$

10. By Statement 10, A1, A4, A5, and A6, we apply the nonce verification rule to derive

$$\text{FA believes that HA believes } (ID_{HA}, ID_{FA}). \tag{Statement 11}$$

11. By Statement 11 and A18, we break the conjunction to obtain

$$\text{FA believes that HA believes } ID_{HA}. \tag{Statement 12}$$

12. By Statement 12, we apply the jurisdiction rule to obtain

$$\text{FA believes } ID_{HA}. \tag{Statement 13}$$

13. By m_{V3}, A1, A4, and A12, we break the conjunction to obtain

$$\text{FA believes that MU believes } <MU \overset{SK}{\longleftrightarrow} FA>. \tag{Statement 14}$$

14. By Statement 14, we apply the jurisdiction rule to obtain

$$\text{FA believes } <\text{MU} \overset{SK}{\longleftrightarrow} \text{FA}>. \qquad \text{(Statement 15)}$$

15. By m_{V4} and A16, we break the conjunction to obtain

$$\text{MU believes that FA believes } <\text{MU} \overset{SK}{\longleftrightarrow} \text{FA}>. \qquad \text{(Statement 16)}$$

16. By Statement 14, 15, 16, and A11, we prove that the process of setting the session key is safe between the MU and the FA.

From the foregoing analysis, we can find a consistent result with assumption A11 and Statement 16. Therefore, this indicates that Assumption A11 is established, and this also proves that the process of setting the session key is safe between the MU and the FA in our proposed scheme.

5. Security Analysis

In the authentication phase of our proposed scheme, we improved the session key ID_{HA} by using symmetric encryption computation, compared with Li's scheme that does not perform any encryption protection. Therefore, the anonymity level of the proposed scheme is even stronger than that of Li's scheme. In other words, the security level increased from C2 to C3 (in [13], the C2 level means that the FA does not know the identity of the anonymous user, and the C3 level means that the attacker does not know the relationship among the MU, FA and HA) Hence, the attacker cannot intercept ID_{HA} and cannot use replay attacks to paralyze the HA. In addition, for the problem of generating the session key in the roaming phase, our approach lets the MU encrypt the calculated session key by using the shared key EC and transmits it to the FA. Therefore, no problems are encountered during transmission. The FA does not need to recalculate the session key, and therefore, the amount of computation is reduced because there is no additional matching of session keys to individual MUs. Finally, the computation of the session key is balanced between the sender and the receiver in the authentication phase. In this section, we show that the proposed scheme can withstand some possible attacks and affords several good security properties.

5.1. Resist Replay Attack

The proposed scheme has a timestamp in each transmission process, including the authentication (V1→V5) and roaming (L1→L2) phases. In addition, V1 and L1 are encrypted by using the shared key EC, and therefore, we can imagine that V1 and L1 are secure channels. Therefore, even if an attacker intercepts the message, the message cannot be broken in this secure channel. This allows our proposed scheme to resist replay attacks.

5.2. Resist Distributed Denial-of-Service Attack

The attacker can intercept the cipher text of message m_1 that contains the timestamp T_{MU} and ID_{HA}. However, the attacker cannot decrypt the cipher text and cannot forge the timestamp T_{MU} and specific object ID_{HA}. Then, the attacker cannot use a distributed denial-of-service attack to attack the HA.

5.3. Achieve High Level of Anonymity

In a wireless environment, messages can be intercepted easily. In [27], the MU sends the authentication message m_1 to the FA in the authentication phase. The message content is not encrypted, and therefore, the attacker easily intercepts ID_{HA} and then determines the relationship among the MA, FA, and HA. When the relationship is known, the level of anonymity of the entire scheme is lowered, and the attacker can successfully use the attacks described in Sections 4.2 and 4.3. In our proposed scheme, when the MU wants to send the message to the FA, it will calculate the shared key EC and then encrypt the message by using EC to achieve the security and integrity requirements. Only the FA possesses the EC, and therefore, other people cannot decrypt this cipher text. Therefore, our scheme can achieve the C3 level requirement of high anonymity.

5.4. Solve Corresponding Problem of Session Key in Roaming Phase

In Li's scheme, when the FA receives the roaming message, it calculates the session key, decrypts the cipher text m_i, and performs a comparison with mac. However, there are in fact hundreds of thousands of people in a wireless network environment, and Li's scheme did not clearly discuss how to calculate the session key in the roaming phase. Each person's session key is not the same, and it did not clarify how to calculate one hundred thousand different session keys or save them in the table. It can be saved as a form, but this may pose some risks, which need to be discussed further. In the proposed scheme, the FA can decrypt the cipher text m_i by using the session key calculated by the MU in the authentication phase. On the other hand, we encrypt the session key by using EC calculated by the MU in the authentication phase. In this manner, our scheme resists data disclosure to attackers, who intercept the session key during the transfer processes. Even if the message is intercepted, it can only reveal the cipher text. Therefore, the proposed scheme solves the corresponding problem of the session key.

5.5. Balanced Calculation of Session Key

The load of session key computation is balanced between the senders and the receivers in the authentication phase. Table 4 shows the balanced calculation of the session key.

Table 4. Balanced calculation of the session key.

Sender	Receiver
V1: MU calculates X = xP and EC = aP_{FA} = abP	V2: FA calculates Y = yP and EC = bA = abP
V2: FA calculates MAC_{FA}	V3: HA calculates MAC_{FA}
V3: HA calculates MAC_{HA}	V4: FA calculates MAC_{HA}
V4: FA calculates sk_i = xY and c_2	V5: MU calculates sk_i = xY and c_2

6. Comparison with Related Works

Table 5 shows that the proposed scheme can resist internal attack, replay attack, and distributed denial-of-service attack for the specific object while maintaining a high level of anonymity. It provides a balanced calculation and solves the issue of session key management. Li's scheme cannot resist replay attack or distributed denial-of-service attack for the specific object while also providing less anonymity of level C2. Li's scheme did not address the problem of session key management as calculated by the FA in the roaming phase. However, our proposed scheme resolves these issues. Our method maintains the advantages and weaknesses of Zhu and Ma's [24] scheme from 2004 and Lee et al.'s [25] scheme from 2006.

Table 5. Comparison with related works.

Secure Item	Li [27]	Lee et al. [25]	Zhu-Ma [24]	Our Scheme
Resist internal attack	Yes	No	No	Yes
Resist replay attack	No	Yes	Yes	Yes
Resist distributed denial-of-service attack for specific object	No	Yes	Yes	Yes
Achieve a high level of anonymity	No	No	No	Yes
Session key providing anonymity and authentication	No	No	No	Yes
Balanced calculation of the session key	Yes	No	No	Yes

7. Conclusions

This study proposes an elliptic-curve-based authentication scheme with roaming service and user anonymity for mobile communication. It overcomes the weaknesses of Li's scheme [27] and provides balanced session key computation in the authentication phase. We use an elliptic curve in the calculations, and therefore, the security performance is good. Although our computational complexity is comparable to that of Li's scheme, our scheme reduces the load of MU calculation by moving this calculation to the HA, which has better computing performance. Finally, the advantages and weaknesses of our scheme are compared with those of other related works, and it demonstrates improved security, anonymity, and resistance to attacks without having additional computational complexity.

Acknowledgments: This work was supported by MOST 105-2221-E-145-002.

Author Contributions: Kai Chain, Wen-Chung Kuo and Jiin-Chiou Cheng conceived and designed the experiments; Kai Chain and Wen-Chung Kuo performed the experiments and analyzed the data; Kai Chain wrote the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Liu, K.H.; Li, J.S.; Wang, C.Y.; Chilamkurti, N.; Vasilakos, A.V. Minimizing multiplayer interactive delay in multihop wireless networks. *Int. J. Commun. Syst.* **2012**, *25*, 1330–1349. [CrossRef]
2. Vavoulas, A.; Vaiopoulos, N.; Varoutas, D.A.; Chipouras, A.; Stefanou, G. Performance improvement of fixed wireless access networks by conjunction of dual polarization and time domain radio resource allocation technique. *Int. J. Commun. Syst.* **2011**, *24*, 483–491. [CrossRef]
3. Li, J.S.; Liu, K.H. A hidden mutual authentication protocol for low-cost RFID tags. *Int. J. Commun. Syst.* **2011**, *24*, 1196–1211. [CrossRef]
4. Tang, H.B.; Liu, X.S. Cryptanalysis of a dynamic ID-based remote user authentication with key agreement scheme. *Int. J. Commun. Syst.* **2012**, *25*, 1639–1644. [CrossRef]
5. Buttyan, L.; Gbaguidi, C.; Staamann, S.; Wilhelm, U. Extensions to an authentication technique proposed for the global mobility network. *IEEE Trans. Commun.* **2000**, *48*, 373–376. [CrossRef]
6. Hwang, K.F.; Chang, C.C. A self-encryption mechanism for authentication of roaming and teleconference services. *IEEE Trans. Wirel. Commun.* **2003**, *2*, 400–407. [CrossRef]
7. Tzeng, Z.J.; Tzeng, W.G. Authentication of mobile users in third generation mobile system. *Wirel. Pers. Commun.* **2001**, *16*, 35–50. [CrossRef]
8. Suzukiz, S.; Nakada, K. An authentication technique based on distributed security management for the global mobility network. *IEEE J. Sel. Areas Commun.* **1997**, *15*, 1608–1617. [CrossRef]
9. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]
10. Lee, C.Y.; Chang, C.C.; Lin, C.H. User authentication with anonymity for global mobility networks. In Proceedings of the IEEE Mobility Conference 2005: The Second Asia Pacific Conference on Mobile Technology, Applications and Systems, Guangzhou, China, 15–17 November 2005.
11. Lin, C.H.; Lee, C.Y. Cryptanalysis of a new authentication scheme with anonymity for wireless environments. In Proceedings of the Second International Conference on Advances in Mobile Multimedia, Bali, Indonesia, 22–24 September 2004; pp. 399–402.
12. Li, C.T. Secure smart card based password authentication scheme with user anonymity. *Inf. Technol. Control* **2011**, *40*, 157–162. [CrossRef]
13. Wan, Z.; Ren, K.; Preneel, B. A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks. In Proceedings of the First ACM Conference on Wireless Network Security, Alexandria, VA, USA, 31 March–2 April 2008; pp. 62–67.
14. Chen, C.L.; Lee, C.C.; Hsu, C.Y. Mobile device integration of a fingerprint biometric remote authentication scheme. *Int. J. Commun. Syst.* **2012**, *25*, 585–597. [CrossRef]
15. Chuang, Y.H.; Tseng, Y.M. Towards generalized ID-based user authentication for mobile multi-server environment. *Int. J. Commun. Syst.* **2012**, *25*, 447–460. [CrossRef]
16. Xie, Q. A new authenticated key agreement for session initiation protocol. *Int. J. Commun. Syst.* **2012**, *25*, 47–54. [CrossRef]

17. Argyroudis, P.G.; Verma, R.; Tewari, H.; O'Mahony, D. Performance analysis of cryptographic protocols on handheld devices. In Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications (NCA2004), Cambridge, MA, USA, 2004; pp. 169–174.
18. Chen, B.L.; Kuo, W.C.; Wuu, L.C. Robust smart-card-based remote user password authentication scheme. *Int. J. Commun. Syst.* **2014**, *27*, 377–389. [CrossRef]
19. Doomun, M.R.; Soyjaudah, K.S.; Bundhoo, D. Energy consumption and computational analysis of Rijndael-AES. In Proceedings of the Third IEEE International Conference in Central Asia on Internet the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007), Tashkent, Uzbekistan, 26–28 September 2007; pp. 1–6.
20. Passing, M.; Dressler, F. Experimental performance evaluation of cryptographic algorithms. In Proceedings of the 3rd IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Vancouver, BC, Canada, 9–12 June 2006; pp. 882–887.
21. Passing, M.; Dressler, F. Practical evaluation of the performance impact of security mechanisms in sensor networks. In Proceedings of the 31st IEEE Conference on Local Computer Networks, Tampa, FL, USA, 14–17 November 2006; pp. 623–629.
22. Syverson, P. A taxonomy of replay attacks. In Proceedings of the 7th IEEE Computer Security Foundations Workshop, Franconia, NH, USA, 14–16 June 1994; pp. 131–136.
23. Wong, D.S.; Fuentes, H.H.; Chan, A.H. The performance measurement of cryptographic primitives on palm devices. In Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC 2001), New Orleans, LA, USA, 10–14 December 2001; pp. 92–101.
24. Zhu, J.; Ma, J. A new authentication scheme with anonymity for wireless environments. *IEEE Trans. Consum. Electron.* **2004**, *50*, 230–234.
25. Lee, C.C.; Hwang, M.S.; Liao, I.E. Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Trans. Ind. Electron.* **2006**, *53*, 1683–1687. [CrossRef]
26. Lee, J.S.; Chang, J.H.; Lee, D.H. Security flaw of authentication scheme with anonymity for wireless communications. *IEEE Commun. Lett.* **2009**, *13*, 292–293.
27. Li, C.T. A more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications. *Inf. Technol. Control* **2012**, *41*, 69–76. [CrossRef]
28. Rivest, R.L.; Shamir, A.; Adleman, L.M. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
29. Deng, Y. Based on BAN logic analysis otway-rees protocol. *Chaohu Coll. J.* **2006**, *78*, 36–37.
30. Li, T.; Liu, X.; Qin, Z. Formal analysis for security of otway-rees protocol with BAN-logic. In Proceedings of the First International Workshop on Database Technology and Applications, Wuhan, Hubei, 25–26 April 2009; pp. 590–593.
31. Li, T.; Liu, X.; Qin, Z.; Zhang, X. An improved security protocol formal analysis with BAN-logic. In Proceedings of the International Conference on Electronic Commerce and Business Intelligence, Beijing, China, 6–7 June 2009; pp. 102–105.